AMENDMENTS TO THE CLAIMS

1. (Currently Amended) In a personal computer having encryption hardware and a processor, a method of storing data on one or more magnetic or optical data storage media in an encrypted form comprising:

storing an identification code in a non-erasable memory during manufacture of the personal computer, wherein said identification code is defined at least in part by information associated with components of said personal computer;

retrieving the identification code from the memory in said personal computer;

receiving user input;

generating a cryptographic key derived at least in part from said identification code and the received user input;

retrieving a checksum from a configuration register in the personal computer;

verifying the generated cryptographic key, wherein verifying comprises determining a checksum of the generated key; and

encrypting and decrypting data, for storage on and retrieval from one of said data storage media using said cryptographic key, wherein the data is transmitted by the processor and is encrypted in the personal computer by the encryption hardware.

2. (Previously Presented) The method of Claim 1, additionally comprising:

retrieving information from a memory location; and

disabling encryption of data routed to one of said data storage media in response to said retrieved information.

3. (Original) The method of Claim 1, wherein said retrieving is performed without intervention by a host processor.

4. (Original) The method of Claim 3, additionally comprising verifying said key, wherein said verifying occurs without intervention of said host processor.

5. (Previously Presented) A method of making a computer comprising:

storing a hardware identifier in a non-erasable memory integrated circuit at the time of manufacture of the computer, wherein the hardware identifier is defined at least in part by information associated with components of said computer;

installing said memory integrated circuit into said computer;

providing a data path to data storage media;

providing a configuration for storing a checksum;

coupling a logic circuit comprising an encryption engine to said data path; and

connecting said memory integrated circuit to said logic circuit, wherein the hardware identifier and user input is used by the encrypting engine for encrypting data that is transmitted to the data storage media and for decrypting data that is retrieved from the data storage media, and wherein the encryption engine verifies the generated cryptographic key using the checksum.

6. (Original) The method of Claim 5, wherein said act of connecting comprises routing a serial data bus from said memory integrated circuit to said logic circuit.

7. (Currently Amended) In a computer system comprising a processor and encryption hardware and at least one data storage device, a method of data storage comprising:

receiving user input;

transmitting data from the processor in the computer system to encryption hardware in the computer system; and

generating a cryptographic key derived at least in part from the received user input and information that is stored in a non-erasable memory in said computer system during manufacture of said computer system;

retrieving a checksum from a configuration register in the computer system;

verifying the generated cryptographic key, wherein verifying comprises determining a checksum of the generated key; and

encrypting and decrypting, in the encryption hardware, user generated data with an encryption process that uses the generated cryptographic key.

8. (Previously Presented) The method of Claim 7, wherein said information is permanently associated with said host computing logic.

9. (Original) The method of Claim 7, wherein said information comprises a multi-bit identification code.

10. (Original) The method of Claim 9, additionally comprising the act of deriving an encryption key at least in part from said identification code.

11. Cancelled

12. (Original) The method of Claim 7, additionally comprising defining said encryption process at least in part from user input to said computer system.

13. (Previously Presented) The method of Claim 1, wherein encrypting data for storage is performed on an encrypting device that is positioned in a data path between a central processing unit and the data storage medium.

14. (Previously Presented) The method of Claim 1, wherein all data that is transmitted to the data storage media is encrypted.

15. (Currently Amended) In a personal computer having encryption hardware and a processor, a method of storing data on one or more magnetic or optical data storage media in an encrypted form comprising:

storing an identification code in a non-erasable memory during manufacture of the personal computer, wherein said identification code is defined at least in part by information associated with components of said personal computer;

retrieving the identification code from the memory in said personal computer;

receiving user input;

generating a cryptographic key derived at least in part from said identification code and the received user input;

retrieving a checksum from a configuration register in the personal computer;

verifying the generated cryptographic key, wherein verifying comprises determining a checksum of the generated key; and

encrypting and decrypting data, for storage on and retrieval from one of said data storage media using said cryptographic key, wherein the data is transmitted by the processor and is encrypted in the personal computer by the encryption hardware, and wherein the encryption hardware is part of a bus-to-bus bridge circuit.

16. (Previously Presented) The method of Claim 1, additionally comprising:

retrieving information from a memory location; and

disabling encryption of data routed to one of said data storage media in response to said retrieved information.

17. (Previously Presented) The method of Claim 1, wherein said retrieving is performed without intervention by a host processor.

18. (Previously Presented) The method of Claim 3, additionally comprising verifying said key, wherein said verifying occurs without intervention of said host processor.